



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11239169 A**(43) Date of publication of application: **31.08.99**

(51) Int. Cl. **H04L 12/54**
H04L 12/58
G06F 13/00

(21) Application number: **10041446**(22) Date of filing: **24.02.98**(71) Applicant: **SUMITOMO ELECTRIC IND LTD**

(72) Inventor: **KOREKAWA NORIO**
NAKAMORI KOSHU
MAEYAMA YOSHIKUNI

(54) FIREWALL DEVICE COPING WITH ELECTRONIC MAIL

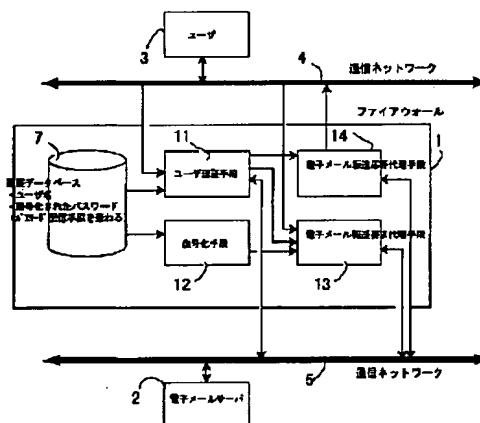
performed by using it.

COPYRIGHT: (C)1999,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To safely utilize an electronic mail server of an internal communications channel from an external communications channel by requesting electronic mail to the electronic mail server corresponding to a request from a user by an electronic mail transfer request representing means after a prescribed procedure and transmitting a response from the electronic mail server to the user.

SOLUTION: Relating to a firewall, after the user 3 connected to a communications network 4 is authenticated by a user authentication means 11, the electronic mail is requested to the electronic mail server 2 corresponding to the request of the user 3 instead of the user 3 by the electronic mail transfer request representing means 13 and the response from the electronic mail server 2 is transmitted to the user 3 by an electronic mail transfer response representing means 14. Since authentication by the user authentication means 11 is performed by a disposable password, even when an intruder eavesdrops the disposable password, authentication can not be



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-239169

(43) 公開日 平成11年(1999) 8月31日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 L 12/54

H 0 4 L 11/20

1 0 1 B

12/58

G 0 6 F 13/00

3 5 1 Z

G 0 6 F 13/00

3 5 1

審査請求 未請求 請求項の数4 O L (全 15 頁)

(21) 出願番号

特願平10-41446

(22) 出願日

平成10年(1998) 2月24日

(71) 出願人 000002130

住友電気工業株式会社

大阪府大阪市中央区北浜四丁目5番33号

(72) 発明者 是川 則雄

大阪府大阪市此花区島屋一丁目1番3号

住友電気工業株式会社大阪製作所内

(72) 発明者 中森 弘修

大阪府大阪市此花区島屋一丁目1番3号

住友電気工業株式会社大阪製作所内

(72) 発明者 前山 欣邦

大阪府大阪市此花区島屋一丁目1番3号

住友電気工業株式会社大阪製作所内

(74) 代理人 弁理士 上代 哲司 (外2名)

(54) 【発明の名称】 電子メール対応ファイアウォール装置

(57) 【要約】

【課題】 従来、外部のネットワーク上のパソコンなどから、ファイアウォールで守られたネットワーク上のメールサーバへ接続するには、機密保護の観点から、容易なことではなかった。

【解決手段】 本発明では、ユーザ認証手段、電子メール転送要求代理手段、および電子メール転送応答代理手段を備えたファイアウォールと電子メールサーバを組み合わせるにより、維持管理が容易で、比較的安価で、かつ、高度な機密性を有するメールシステムを備えた、ファイアウォール装置を構築できる。

1

【特許請求の範囲】

【請求項1】 複数の通信ネットワークに接続されており、その内のある通信ネットワーク（4）からの通信を選択的に別の通信ネットワーク（5）に伝送するファイアウォール装置において、

通信ネットワーク（4）に接続されているユーザ（3）を、使い捨てパスワードを用いて認証するユーザ認証手段（11）と、ユーザ（3）の電子メールの要求に応じて通信ネットワーク（5）に接続されている電子メールサーバ（2）に対して電子メールに関する要求を代行する電子メール転送要求代理手段（13）と、電子メールサーバ（2）からの応答をユーザ（3）に送信する電子メール転送応答代理手段（14）とを有し、通信ネットワーク（4）に接続されているユーザ（3）の認証を行なった後に、そのユーザ（3）の代わりにユーザ（3）からの要求に応じて電子メールサーバ（2）に電子メールの要求を行い、電子メールサーバ（2）からの応答をユーザ（3）に送信することを特徴とする電子メール対応ファイアウォール装置。

【請求項2】 複数の通信ネットワークに接続されており、その内のある通信ネットワーク（4）からの通信を選択的に別の通信ネットワーク（5）に伝送するファイアウォール装置において、

通信ネットワーク（4）に接続されているユーザ（3）から使い捨てパスワードを受け取り、この使い捨てパスワードを通信ネットワーク（5）に接続されている認証サーバ（8）に送信してユーザ認証の可否を問い合わせるユーザ認証問合せ手段（15）と、

ユーザ（3）の電子メールの要求に応じて通信ネットワーク（5）に接続されている電子メールサーバ（2）に対して電子メールに関する要求を代行する電子メール転送要求代理手段（13）と、

電子メールサーバ（2）からの応答をユーザ（3）に送信する電子メール転送応答代理手段（14）とを有し、通信ネットワーク（4）に接続されているユーザ（3）が認証サーバ（8）によって認証された後に、そのユーザ（3）の代わりにユーザ（3）からの要求に応じて電子メールサーバ（2）に電子メールの要求を行い、電子メールサーバ（2）からの応答をユーザ（3）に送信することを特徴とする電子メール対応ファイアウォール装置。

【請求項3】 請求項1または請求項2に記載の電子メール対応ファイアウォール装置において、さらに、ユーザ（3）の電子メールサーバ（2）に対するパスワードRを記憶するパスワード記憶手段、または、パスワードRを通信ネットワーク（5）に接続されているパスワード記憶装置から取得するパスワード取得手段（16）を有し、

通信ネットワーク（4）に接続されているユーザ（3）の認証を行なった後は、パスワード記憶手段またはパス

2

ワード取得手段（16）から得たパスワードRを使って電子メールサーバ（2）に対する電子メールの要求を行なうことを特徴とする電子メール対応ファイアウォール装置。

【請求項4】 請求項3に記載の電子メール対応ファイアウォール装置において、さらに、暗号化されたパスワードVを平文のパスワードWに戻す復号化手段を有し、パスワード記憶手段またはパスワード取得手段から得たパスワードVを平文のパスワードWに戻したのちに、その平文のパスワードWを使って電子メールサーバ（2）に対する電子メールの要求を行なうことを特徴とする電子メール対応ファイアウォール装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、不特定の第三者にも利用される通信チャンネル（以下、外部通信チャンネル）と特定の関係者しか利用されない（不特定の第三者には利用されない）通信チャンネル（以下、内部通信チャンネル）の間に設けるファイアウォール装置（以下、ファイアウォールと略称する）に関するものである。特に、内部通信チャンネルに接続されている電子メールサーバに、外部通信チャンネルからアクセスを安全に行ないたい場合に用いると好適である。

【0002】

【従来の技術】 電子メールは、インターネットの拡大と共に普及が進んでおり、一企業内での従業員相互間の連絡にもしばしば使われるようになってきている。インターネット関連で市販されているツールを、企業内のみの情報伝達に流用することも広く行なわれており、イントラネットと呼ばれている。イントラネットを使って、電子メールを従業員相互間でやりとりする場合の構成を図3に示す。図3において、22はイントラネットを構成する通信チャンネルである。図3では、便宜上リング状に書いてあるが、通信チャンネルを構成する通信機器をすべてリング状に接続する必要はなく、ツリー状、スター状等、各種のトポロジで接続することができる。21は電子メールサーバである。電子メールを使用したい従業員等、すなわち、ユーザは、自分の操作するコンピュータ（以下、ユーザ用コンピュータ）を使って、電子メールサーバにアクセスする。具体的には、各ユーザがユーザ用コンピュータ23、24、…を使って送信した電子メールは、一旦電子メールサーバ21に蓄えられ、必要に応じて、取り出される。電子メールを電子メールサーバ21から取り出す際は、ユーザ名、パスワードを電子メールサーバに与えることで、正当な利用者であることを示す。すなわち、ユーザ名とパスワードの組合せによって、ユーザの認証が行なわれる。22は、企業内（所定の敷地や、建物）に設置されている。不正な第三者（以下、侵入者）が22に流れている情報を不正に入手しようと思っても、その企業内に立ち入ることができ

3

ないため、22に接続することができない。すなわち、企業内への立ち入りを制限することによって、物理的に22は安全が保たれている。かかる場合は、電子メールのやりとりにおいても、さしたる機密保護のための処置は必要がない。機密保護のための処理が不要なので、各ユーザは、パスワードや電子メールを暗号化する手間を省くことができ、簡便かつ能率よく、電子メールを利用することができる。そのため、22に流れるパスワードは、暗号化されていない平文のままである。

【0003】次に、イントラネット22を外部通信チャンネルに接続する場合の構成を図4に示す。外部通信チャンネルは、例えば、公衆回線やインターネットであり、侵入者の盗聴や攻撃はありうる。従って、イントラネット22の内容がそのまま外部通信チャンネル28に流出したり、外部通信チャンネル28の内容が勝手にイントラネット22に流れこんだりしないように、ファイアウォール20を設ける。ファイアウォール20は、真に意図した通信のみをイントラネット22と外部通信チャンネル28の間で通過させ、それ以外の通信を遮断する働きを持つ。また、ファイアウォール20は、外部の侵入者からの根気良い攻撃に耐える必要がある。イントラネットの外のユーザに対し、電子メールサーバ21の内容に、ファイアウォール20を経て接続できないようにしてしまうと不便であるので、予め決められた種類の通信（例えば、電子メールの要求のみ）を、外部通信チャンネル28からイントラネット22へ通過させる設定が考えられる。安全さが多少は犠牲になるが、電子メールを外部ネットワークから読み出すことができるようになる。ただし、電子メールサーバ21へのユーザ名とパスワードが平文のままでは、外部通信チャンネル28を盗聴する侵入者によって簡単に悪用されてしまう。そこで、暗号化手続きを利用して、電子メールサーバ21に対する認証を行なわなければならない。暗号化手続きによる認証としては、例えば、RFC1939（ftp://ds.internic.net/rfc/rfc1939.txt）に規定されているPOP3（Post Office Protocol-version 3）のAPOPコマンドを使用することができる。この様にすれば、電子メールを外部ネットワークから読み出すことができるようになる（従来技術a）。また、ファイアウォールに対する安全性を高めるために、暗号化手続きによる認証をファイアウォールにも適用するという構成（以下、従来技術b）も取り得る。すなわち、電子メールサーバへの電子メールの要求に先立って、まず、ファイアウォールに対して暗号化手続きによる認証を行なうという構成である。

【0004】

【発明が解決しようとする課題】従来技術aで説明したように、APOPコマンドを使えば、電子メールサーバへのパスワードの盗聴そのものに対する耐性は得られ

4

る。しかし、電子メールに関する要求はファイアウォールを通過するように設定されているので、安全さが多少犠牲になっている。たとえば、侵入者は外部ネットワークを盗聴していると、電子メールの要求の通信だけはファイアウォールを通過することを発見しうる。そして、侵入者が電子メールの要求の通信を外部ネットワークから流し込むと、その通信はファイアウォール20を抜けてイントラネット22に入ることになる。すると、電子メールサーバがその電子メールの要求を認証しなくても（無視しても）、電子メールの要求が大量に流れれば、イントラネット22の伝送容量を上回った時点で、通信障害が発生する。このようにして、イントラネット22を使った企業内活動を停止させる事態が生じうる。つまり、強い破壊の意図を持った侵入者に対しては防御ができない。これは、POP3のAPOPコマンドの規約そのものが、電子メールサーバのみを考慮において構築されたために内在することとなった、システム構築上の限界である。

【0005】従来技術bでは、ファイアウォールに対する認証を済ませなければ、電子メールに関する通信も通過できないので、ファイアウォール越しの攻撃は防御できる。しかし、電子メールサーバへの電子メールの要求に先立って、まず、ファイアウォールに対して暗号化手続きによる認証を行なわなければならない。すなわち、ファイアウォールへの認証手続きと、POP3への認証手続きを共に行なわねばならず、煩雑である。また、ユーザ登録の維持や認証手続きの管理の手間も二重に必要になり、管理コストの増大という欠点が生じる。

【0006】以上の様に、従来技術による外部ネットワークから内部ネットワークの電子メールの読み出しは、本質的に安全性に欠ける（従来技術a）か、煩雑な手続きや管理コストの増大（従来技術b）という問題が避けられなかった。なお、APOPコマンドはPOP3のオプションであり、これが電子メールサーバには実装されているとは限らない。イントラネットは、最初は簡便な方法で構築し、その後は管理者の熟達や利用者数の増大に応じて発展させるのが普通である。APOPコマンドのない簡便で入手しやすい電子メールサーバを使ってイントラネットを構築すると、そのままでは後に外部ネットワークに接続できないというのでは困る。仮に、APOPコマンドのある電子メールサーバに交換するとなると、交換の費用や手間等の出費が嵩んでしまう。また、そもそもAPOPコマンドを実装した電子メールサーバは実はあまり市販されていないので、現実には、上記に述べたシステムすら構築しにくいという欠点もある。本願発明は、これらの欠点を解消して、安全に外部通信チャンネルから内部通信チャンネルの電子メールサーバを利用する手段を提供するものである。

【0007】

【課題を解決するための手段】図1に請求項1と3と4

5

を組み合わせたファイアウォールの構成を示す。4は外部通信チャンネルに相当する通信ネットワークであり、5は内部通信チャンネルに相当する通信ネットワークである。3は通信ネットワークに接続されているユーザである。言うまでもなく、通信ネットワーク4に接続されているのは、実際には、ユーザ3が操作する個人用コンピュータ（不図示）であり、ユーザ3はこの個人用コンピュータを介して通信ネットワーク4を使用する。ここでは、発明の本質を簡潔に表すために、途中に介在する個人用コンピュータを省いて、ユーザ3が通信ネットワークを使用するものとして説明する。2は通信ネットワーク4に接続されている電子メールサーバ2であり、通信ネットワーク5に接続されている他の装置やユーザからの要求に応じて、受信済みの電子メールを回答したり、電子メールを発信する処理を行なう。ユーザ3は電子メールサーバ2から、自己の電子メールを得たいと意図している。

【0008】図2に請求項2と3と4を組み合わせたファイアウォールの構成を示す。8は通信ネットワーク5に接続された認証サーバであり、通信ネットワーク5に接続された他の装置からの要求に応じて、ユーザの認証を行なう。7は、認証サーバ8の有する認証データベースである。

【0009】請求項1によるファイアウォールは、通信ネットワーク4に接続されているユーザ3を、使い捨てパスワードを用いて認証するユーザ認証手段11と、ユーザ3の電子メールの要求に応じて5に接続されている電子メールサーバ2に対して電子メールに関する要求を代行する電子メール転送要求代理手段13と、電子メールサーバ2からの応答をユーザ3に送信する電子メール転送応答代理手段14と、を有することを特徴とする。なお、7は、ユーザ認証手段11において必要となるユーザ名等の認証情報を記憶する認証データベースである。請求項2によるファイアウォールは、通信ネットワーク4に接続されているユーザ3から使い捨てパスワードを受け取り、この使い捨てパスワードを通信ネットワーク5に接続されている認証サーバ8に送信してユーザ認証の可否を問い合わせるユーザ認証問い合わせ手段15と、ユーザ3の電子メールの要求に応じて通信ネットワーク5に接続されている電子メールサーバ2に対して電子メールに関する要求を代行する電子メール転送要求代理手段13と、電子メールサーバ2からの応答をユーザ3に送信する電子メール転送応答代理手段14と、を有することを特徴とする。請求項3によるファイアウォールは、請求項1又は2に加えてさらに、ユーザ3の電子メールサーバ2に対するパスワードRを記憶するパスワード記憶手段、または、パスワードRを通信ネットワーク5に接続されている認証データベース7（パスワード記憶装置）から取得するパスワード取得手段16を有することを特徴とする。なお、パスワードはユーザの認証

6

に必要な情報と共に記憶することもできるので、図1と2では、認証データベースの中にパスワードも記憶されているものとして図示している。図2においては、認証データベース7の中のパスワードは、認証サーバ8を経由してパスワード取得手段16に送られる。請求項4によるファイアウォール装置は、請求項1と3、又は、2と3に加えてさらに、暗号化されたパスワードVを平文のパスワードWに戻す復号化手段12を有することを特徴とする。なお、図1と図2では、説明の便宜上、ファイアウォール1に接続する通信ネットワークが2つの場合を示したが、本発明は2つの通信チャンネルに限られることはなく、より多くの外部通信チャンネルや内部通信チャンネルを互いに接続する構成にすることも可能である。

【0010】

【作用及び効果】請求項1によるファイアウォールは、ユーザ認証手段11によって通信ネットワーク4に接続されているユーザ3の認証を行なった後に、電子メール転送要求代理手段13によってそのユーザ3の代わりにユーザ3からの要求に応じて電子メールサーバ2に電子メールの要求を行い、電子メール転送応答代理手段14によって電子メールサーバ2からの応答をユーザ3に送信する。ユーザ認証手段11による認証は使い捨てパスワードにより行なわれるので、仮に侵入者がその使い捨てパスワードを盗聴したとしても、その使い捨てパスワードを使って侵入者が認証を行なうことができない。一方、電子メールサーバ2にとっては、ユーザ3からの電子メールの要求は通信ネットワーク5に接続されている電子メール転送要求代理手段13から送られ、ユーザ3への電子メールに関する回答は通信ネットワーク5に接続されている電子メール転送応答代理手段14に送るだけなので、これは通信ネットワーク5に接続されている他のユーザとのやりとりと変わらない。すなわち、請求項1の発明によれば、電子メールサーバを改変することなく、盗聴されても安全な方法による認証手続きを経た後に、外部通信チャンネルから電子メールサーバにアクセスできるようになる。そのため、

【0011】 従来技術aにおける、破壊の意図を持つ侵入者による電子メールの要求通信が外部通信チャンネルから内部通信チャンネルに無制限に流れ込む危険が、未然に回避できる。

【0012】 従来技術bにおける、ファイアウォールと電子メールサーバの双方に対する認証手続きに比べ、認証の手間や管理の手間が減る。

【0013】 電子メールサーバは、イントラネット用に既に導入したものがそのまま使える。そのため、新たな電子メールサーバを購入する費用や、使い方に熟達する手間が不要となる。また、電子メールサーバの交換する場合に生じる、イントラネット内部に対する電子メールのサービスの中断も避けられる。これらの点で、経済

的な利点大きい。

【0014】請求項2によるファイアウォールは、ユーザ認証問い合わせ手段15が通信ネットワーク5に接続されている認証サーバ8に依頼して、通信ネットワーク4に接続されているユーザ3を認証した後に、電子メール転送要求代理手段13によってそのユーザ3の代わりにユーザ3からの要求に応じて電子メールサーバ2に電子メールの要求を行い、電子メール転送応答代理手段14によって電子メールサーバ2からの応答をユーザ3に送信する。すなわち、請求項2の発明によれば、ファイアウォールとは別に用意した認証サーバに認証処理を行なわせることができる。そのため、請求項1の発明の効果に加えて、

【0015】ファイアウォールが外部からの攻撃に耐えられなくなつて万一故障したとしても、認証サーバおよび認証サーバに蓄えている個々のユーザの認証データはそのまま残るので、より安全である。

【0016】複数の外部ネットワークを繋ぐためにファイアウォールを複数設けた場合など、認証結果が複数の場所で必要な場合、個々に認証データを記憶し、認証処理を行なわなくてすむ。つまり、個々のファイアウォールそれぞれに認証データを置いて認証処理を行なう場合に比べると記憶場所の削減や管理の一体化ができる。

【0017】請求項3によるファイアウォールは、通信ネットワーク4に接続されているユーザ3の認証を行なった後は、認証データベース7（パスワード記憶手段）またはパスワード取得手段16から得たパスワードRを使って電子メールサーバ2に対する電子メールの要求を行なう。すなわち、請求項3の発明によれば、パスワードを外部通信チャンネルからではなく、ファイアウォールから又は、内部通信チャンネルから転送させることができる。そのため、請求項1または2の発明の効果に加えて、

【0018】ファイアウォールに対する認証とは別に、電子メールサーバの認証用のパスワードを、外部通信チャンネルにいるユーザが入力する手間を省ける。

【0019】パスワードを憶える手間を節約するため、ユーザが電子メールサーバに対してだけでなく当該ユーザが利用する複数の計算機に同一のものを使っている場合がある。外部通信チャンネルにいるユーザがパスワードを入力すると、覗き見等によりパスワードが漏洩し、別の計算機に悪用される可能性も生じる。本発明によれば、電子メールサーバ用のパスワードは当該企業の外に出る場合が全くなくなるので、安全性が高まる。

【0020】請求項4によるファイアウォールは、認証データベース（パスワード記憶手段）またはパスワード取得手段16から得たパスワードVを平文のパスワードWに戻したのちに、その平文のパスワードWを使って電子メールサーバ2に対する電子メールの要求を行なう。

すなわち、請求項4の発明によれば、認証データの一部として記憶しておくパスワードを暗号化しておける。そのため、請求項3の発明の効果に加えて、

【0021】認証データそのものを見るだけではパスワードが判らないので、認証データにアクセスする他のユーザや管理者からの秘匿の必要性がなくなり、認証データへのアクセスを細かく制限する手間を省ける。

【0022】

【実施例】 まず、本発明によるファイアウォールを使用するときの、ネットワークの接続を図5に例示する。30は本発明によるファイアウォールであり、通信チャンネル36と通信チャンネル37に接続されている。ルータ34と35は、通信チャンネルの経路を選択する装置である。ルータ34を介してインターネット39は通信チャンネル36に接続され、ルータ35を介して社内の別のネットワーク38は通信チャンネル37に接続されている。通信はルータを経由して行なうことができるので間接的にはあるが、ユーザ29は通信チャンネル36に接続され、電子メールサーバ31は通信チャンネル37に接続されていることになる。請求項2による発明の場合を図示するために、認証サーバ32が、通信チャンネル37に接続されている。請求項1による発明の場合は、ユーザ29の認証はファイアウォール30自身が行なうので、認証サーバをファイアウォールとは別に設ける必要はない。請求項1または2における使い捨てパスワードは、正規の認証に使用した後は使えなくなる性質のものである。例えば、一定期間だけ使用できるパスワードや1回だけ使用できるパスワード（ワンタイムパスワード）で実施すれば良い。以降では、ワンタイムパスワードの場合で説明する。図5において、ユーザ29が電子メールサーバ31から自己の電子メールを取り出すには、次のような手続きを経る。

【0023】1、予め、ユーザ29は自分のユーザ名と電子メールサーバ31に対するパスワードWを認証サーバ32上のデータベースに登録しておく。この際、電子メールサーバ31に対するパスワードは暗号化したパスワードVに登録しておく。

【0024】2、ユーザ29はワンタイムパスワード発生装置33を使って、ファイアウォール30に認証させる。後の処理を簡潔に進めるため、この際、電子メールサーバ31で必要となる情報も合わせてファイアウォールに伝えておくが良い。例えば、電子メールサーバ31における電子メールアドレスと、ネットワーク上でのファイアウォール名を%で結合して、user@office.company.co.jp%fw.company.co.jpというフォーマットで送る。

【0025】3、ファイアウォール30は、ユーザ29から受信したワンタイムパスワード等の情報を認証サーバ32に送り、認証を求める。

【0026】4、認証サーバは認証を行なう。認証が成

功したら（正規のユーザと認められたら）、認証サーバデータベースから暗号化されたパスワードVを取出し、「認証が成功した」旨と、この暗号化パスワードVをファイアウォール30に回答する。

【0027】5、ファイアウォール30は、暗号化パスワードVを平文のパスワードWに復号し、ユーザのメールアドレス等と共に電子メールサーバ31に送って、電子メールのやりとりを行なうセッションを開設する。

【0028】6、以降は、ファイアウォール30は、ユーザ29からの電子メールの要求を通信チャンネル36から出されたのと同じ形式に直して電子メールサーバ31に伝え、電子メールサーバ31からの回答をユーザ29に伝える。

【0029】なお、請求項1の発明は、認証サーバ32にいちいち問い合わせるのではなく、ファイアウォール30の中で認証処理を行なうようにすれば実施できる。本発明のファイアウォール30は、各構成要素をハードウェアによって実施する他、計算機上で動作するソフトウェアによって実施することもできる。計算機としては、ファイアウォール専用の装置を使用する以外に、パソコンやワークステーション等の汎用の計算機を使用することもできる。パソコンやワークステーションを使用するときは、複数のプロセスを並行して動作させるオペレーティングシステム（例えば、UNIX）を採用し、そのオペレーティングシステムの中心部分（カーネル）と、その中心部分を補助するアプリケーションソフト（デーモンプロセス）に本発明に必要な機能をそれぞれ分担させて実施すると好適である。本発明を実施するためのデーモンプロセスを以降は、POP3 proxyデーモンと呼ぶことにする。本発明をワークステーションで実施するときの、ワークステーション40の構成を図6に示す。請求項2と3と4を、ワークステーションで動作するソフトウェアの処理フローを図7以降に示す。

【0030】図6において、CPU（マイクロプロセッサ）41は、RAM（ランダムアクセスできる読み書き可能なメモリ）43に格納されたプログラムを、RAM43と磁気ディスク42を作業領域として使用しながら実行する。65はブートROM（リードオンリーメモリ）である。CPU41は、電源立ち上げ時にブートROM上のプログラムに従って、磁気ディスク42に格納されたプログラムをRAM43に転送し、以降はRAM43上でプログラムを実行する。CPU41は、イーサネットインターフェイス45を使って通信チャンネル47と通信し、イーサネットインターフェイス46を使って通信チャンネル48と通信する。なお、キーボードとディスプレイは、ワークステーション40がファイアウォールとして機能する際には本質的に不要なので、図から省いてある。

【0031】図7は、イーサネットインターフェイス45に通信が来たときにカーネルで実行すべき処理のフロ

ーを示している。この処理は、イーサネットインターフェイス45がCPU41に割り込みを掛けることによって起動される（S701）。S702は、イーサネットインターフェイス45からイーサネットパケットを読み出す処理である。イーサネットパケットとして、各種のプロトコルのパケット、あるいは、電氣的な雑音により欠損したパケットが読み出される。本実施例のファイアウォールでは、正規のIPパケットのみを通過させたいので、S703でIPパケットか否かを判別し、IPパケットではないものをS704で廃棄している。S705は、IPパケットに付随するプロトコル番号、ポート番号、IPアドレス等のパケット情報を参照する処理である。ここで得たパケット情報を用いてS706以降の処理が行なわれる。S706では、処理対象となっているIPパケットを、通信チャンネル48に通過させる、すなわち、フィルタリングするかを判断する。どのような種類のIPパケットをフィルタリングするかは、フィルタリング情報データベースS707に蓄えてある。フィルタリングしないIPパケットはS708で廃棄する。フィルタリングするIPパケットはS709で、自分宛て（ファイアウォール宛て）か否かを判断する。ファイアウォール宛てで無いならば、単に通信チャンネル48に中継すれば良いパケットなので、S710で通信チャンネル48に適合する形にIPパケットを構築し、S711で経路情報データベースS712を参照してIPパケットの送り先情報を追加して、S713でイーサネットインターフェイス46へイーサネットパケットを書込む。

【0032】一方、S709で、ファイアウォール宛てと判断されたならば、S714以降の処理に進む。単に通信チャンネル48を通過させるのではなく、ファイアウォールで独自の処理が必要となるのは、本発明による電子メールだけでなく、FTP（File Transfer Protocol）、やTELNET（Telnet Protocol）の場合もある。これらは、パケット情報の中のポート番号によって区別できる。S714で、FTPに関するIPパケットと判断された場合は、S715でFTP proxyデーモンにそのパケットを渡す。S716で、TELNETに関するIPパケットと判断された場合は、S717でTELNET proxyデーモンにそのパケットを渡す。S718で、POP3に関するIPパケットと判断された場合は、S719でPOP3 proxyデーモンにそのパケットを渡す。S720で、開設済みのセッションと判断された場合は、そのセッションを開設しているアプリケーションにそのパケットを渡す。アプリケーションには、たとえば、FTP proxyデーモン、TELNET proxyデーモン、POP3 proxyデーモンがある。これらのアプリケーションには、通常は、S715、S716、S717でそれぞれIPパケットを渡さ

れるが、認証サーバとの通信等を行なうためのセッションを開設した際はそのセッションに関するIPパケットはS721で渡される。S720で、開設済みセッションにも該当しない場合は、そのIPパケットに対応する処理が無いので、S722でそのパケットを廃棄する。S723は、カーネルの処理を終えた後のリターンを示している。すなわち、S701からの割り込みが処理の前の状態に復帰する。なお、S715、S717、S719、S721において、カーネルからIPパケットを各アプリケーションに渡すのは、オペレーティングシステムに用意されているプロセス間通信の機能を利用すれば良い。S715やS717によって実現されるFTPやTELNETに関するファイアウォールの機能は公知技術なので説明を省く。

【0033】図8は、図7のカーネルからのIPパケットを受け取るPOP3 proxyデーモンの処理フローである。S801は、図7のS719又はS721からのIPパケットを受け取る処理である。このIPパケットは、POP3に関するものに限られるので、以降ではPOP3パケットと呼ぶことにする。電子メールサーバに対してログインを済ませて、電子メールに関する要求をだせる状態になっているかによって、以降の処理は異なる。S802は、そのIPパケットのユーザに関して、電子メールサーバへのログインが既に行なわれているかを判断する。もし、ログイン済みならば、ユーザから来たそのPOP3パケットを電子メールサーバに中継すれば良い。具体的には、S803で通信チャンネルBに適合する形にIPパケットを構築し、S804でカーネルに対してそのIPパケットを送信する要求を行なう。送信要求とは、具体的には、カーネルをソフトウェアによる割り込みで起動し(図7のS724)、S711、S713の処理を行なわせる。その後は、S723でカーネルからリターンし、図8のS804の次に進む。

【0034】S801で受け取ったPOP3パケットのユーザに関して電子メールサーバへのログインが済んでいないならば、S802の後はS805に進む。S805ではPOP3パケットの中身を見て、以降の認証及びログイン処理を行なうべきか判断する。すなわち、ワンタイムパスワードと「電子メールアドレス%ファイアウォール名」という内容になっているかを判断する。もし、これらの内容が揃っていなければ、認証ができないのでS819でそのPOP3パケットを廃棄する。一方、これらの内容が揃っていれば、認証及びログイン処理に進む。

【0035】S806では、POP3パケットに含まれる電子メールアドレスのユーザ名とワンタイムパスワードを取出し、S808で認証サーバに送って、S809で認証結果を得る。認証サーバへの問い合わせと回答受領のために、専用のセッションをS807で開設し、S

10で閉じている。後述の図9のS920を経由して、カーネルはこの回答を、S809に渡している。認証サーバで行なわれる、ワンタイムパスワードを使った認証は、公知の技術を使うことができる。たとえば、文献Neil Haller, "The S/KEY One-Time Password System" Proceedings of the ISOC symposium on Network and Distributed System Security, February 1994, San Diego, CAや、Neil Haller, The S/KEY One-Time Password System, RFC1760, Bellcore, February 1995にその説明がある。

【0036】S811では、認証サーバからの回答を判断し、もし、「認証成功」でないならば、正規なユーザからのものではないので、S812でそのパケットを廃棄する。一方、「認証成功」ならば、正規のユーザからかもしれない。そこで、S813では認証サーバが認証結果と共に回答した暗号化パスワードを復号化して平文のパスワードに直し、S814ではユーザ名と平文のパスワードを使用して電子メールサーバにログインする。なお、パスワードの暗号化と復号化は、公知の技術を使うことができる。たとえば、文献US National Bureau of Standards, "Data Encryption Standard", Federal Information Processing National Bureau of Standards, "Federal Information Processing Standards (FIPS) Publication 46, January 1977にその説明がある。

【0037】電子メールサーバの状況により(たとえば、ログイン済みのユーザの数が、システムの限界に達しているとき)、ログインに失敗することがある。その場合は、S815からS816に進んで、そのパケットを廃棄する。一方、電子メールサーバへのログインが成功したときは、S817で、ログインに成功した旨を作業領域に記憶し、S818ではユーザに対してはプロンプト(次の入力を行なっても良いという旨のメッセージ)を送る。なお、請求項1の発明を実施するときは、認証に必要なデータベース7の内容を磁気ディスク42に蓄えておき、そのデータベースを使って認証処理を行なうことをS806～S810の代わりに行なえば良い。

【0038】図7と図8は、通信チャンネル47からイーサネットパケットが送られてきたときの処理であるが、通信チャンネル48からイーサネットパケットが送られてきたときのときも類似の処理となる。カーネルのすべき処理を、図8の処理フローとほぼ同じである。異

なる点は、通信の向きが逆なので、S901はイーサネットインターフェイス46からの割り込みで起動され、S902ではイーサネットインターフェイス46からイーサネットパケットを読み出すこと、S913ではイーサネットインターフェイス45にイーサネットパケットを書き込むこと、S910やS911では通信チャンネル47に適合する形でIPパケットの構築や送り先が決定されること、S919とS921でパケットを渡す相手が図10に示すPOP proxyデーモンであること、である。

【0039】図10は、通信チャンネル48から通信チャンネル47に、電子メールに関するパケットを渡すためのPOP proxyデーモンのフローである。オペレーティングシステム上には、図8のPOP proxyデーモン、も、図10のPOP proxyデーモン、も、共に存在している。開設済みのセッションに関するPOP3パケットを受け取って、中継する点は、同様の動作となるので、S801からS804までの処理と、S1001からS1004までの処理はほぼ同じである。ただし、S1003では通信チャンネル47に適合する形でIPパケットが構築され、S1004は通信チャンネル47に送信するため図9のS924以降の処理を呼び出す点が異なる。本実施例では、内部通信チャンネルにいるユーザが、外部通信チャンネルにある電子メールサーバを利用しない場合を例示しているのので、S805からS818までに相当するユーザ認証やログイン処理をせずに、S1005では単にパケットを廃棄している。なお、電子メールサーバの利用を終えるために、ユーザから電子メールサーバに終了を示すコマンドを送った後は、電子メールサーバからユーザに終了した旨のメッセージ（ログアウトの応答）が返される。S1006でこのログアウトの応答を検出したときは、S1007で、当該ユーザの電子メールサーバへのログインが成功した旨の記憶（S817で記憶した内容）を消去する。

【0040】以上の説明から判るように、本発明を構成するユーザ認証問合せ手段15は、S807からS810で実施されている。電子メール転送要求代理手段13は、通信チャンネル4からのパケットがS702、S719、S801、S804、S724、S713を経て通信チャンネル48に送信されることで実施されている。電子メール転送応答代理手段14は、通信チャンネル48からのパケットがS902、S919、S1001、S1004、S914、S913を経て通信チャンネル47に送信されることで実施されている。パスワード取得手段16は、S809で認証サーバからパスワードを受け取ることで実施されている。復号化手段12は、S813で、暗号化パスワードを復号する処理で実施されている。ユーザ認証手段11は、S807からS810における、認証サーバ8への問い合わせの代わりに、認証処理を行えば実施できる。その際、認証に必

要なデータと共に、電子メールサーバへのパスワードを磁気ディスク42に蓄えておけば、磁気ディスク42がパスワード記憶手段の実施例となる。

【0041】本発明のファイアウォールを図5から図10に記載の具体例を用いて説明してきたが、本発明の実施はこの実施例に限られるものではない。上述の説明を参照すればこの実施例以外の代替例、変形例、変更例は当業者には容易に考えつくものと思われる。

【図面の簡単な説明】

10 【図1】本発明の構成を示す第1のブロック図

【図2】本発明の構成を示す第2のブロック図

【図3】イントラネットを用いた電子メールシステム概念図

【図4】イントラネットを外部通信チャンネルへ接続した電子メールシステム概念図

【図5】本発明を実施したファイアウォールの実施例

【図6】本発明を実施したファイアウォールのハードウェア構成

20 【図7】本発明を実施したファイアウォールのカーネル処理のフローチャート（外部ユーザがファイアウォールに対して接続要求した場合）

【図8】本発明を実施したPOP3 proxyデーモンの電子メール転送要求処理のフローチャート（外部ユーザがファイアウォールに対して接続要求した場合）

【図9】本発明を実施したファイアウォールのカーネル処理のフローチャート（電子メールサーバがファイアウォールに対して接続要求した場合）

30 【図10】本発明を実施したPOP3 proxyデーモンの電子メール転送要求処理のフローチャート（電子メールサーバがファイアウォールに対して接続要求した場合）

【符号の説明】

1：ファイアウォール

2：電子メールサーバ

3：ユーザ

4：通信ネットワーク

5：通信ネットワーク

7：認証データベース

8：認証サーバ

40 11：ユーザ認証手段

12：復号化手段

13：電子メール転送要求代理手段

14：電子メール転送応答代理手段

15：ユーザ認証問合せ手段

16：パスワード取得手段

20：ファイアウォール

21：電子メールサーバ

22：イントラネット

23：ユーザ用コンピュータ

50 24：ユーザ用コンピュータ

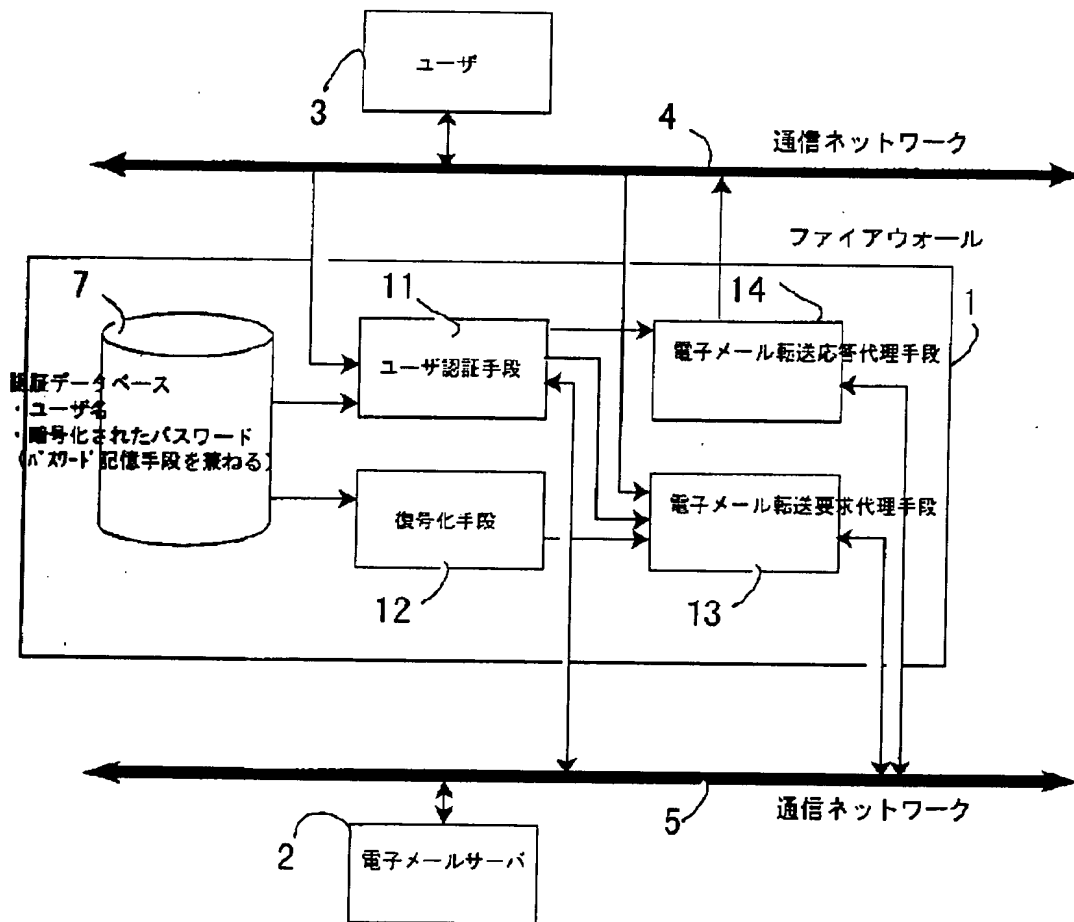
15

- 25 : ユーザ用コンピュータ
 26 : ユーザ用コンピュータ
 27 : 外部ユーザ用コンピュータ
 28 : 外部通信チャンネル
 29 : 外部ユーザ
 30 : ファイアウォール
 31 : 電子メールサーバ
 32 : 認証サーバ
 33 : ワンタイムパスワード発生装置
 34 : ルータ
 35 : ルータ
 36 : 通信チャンネル

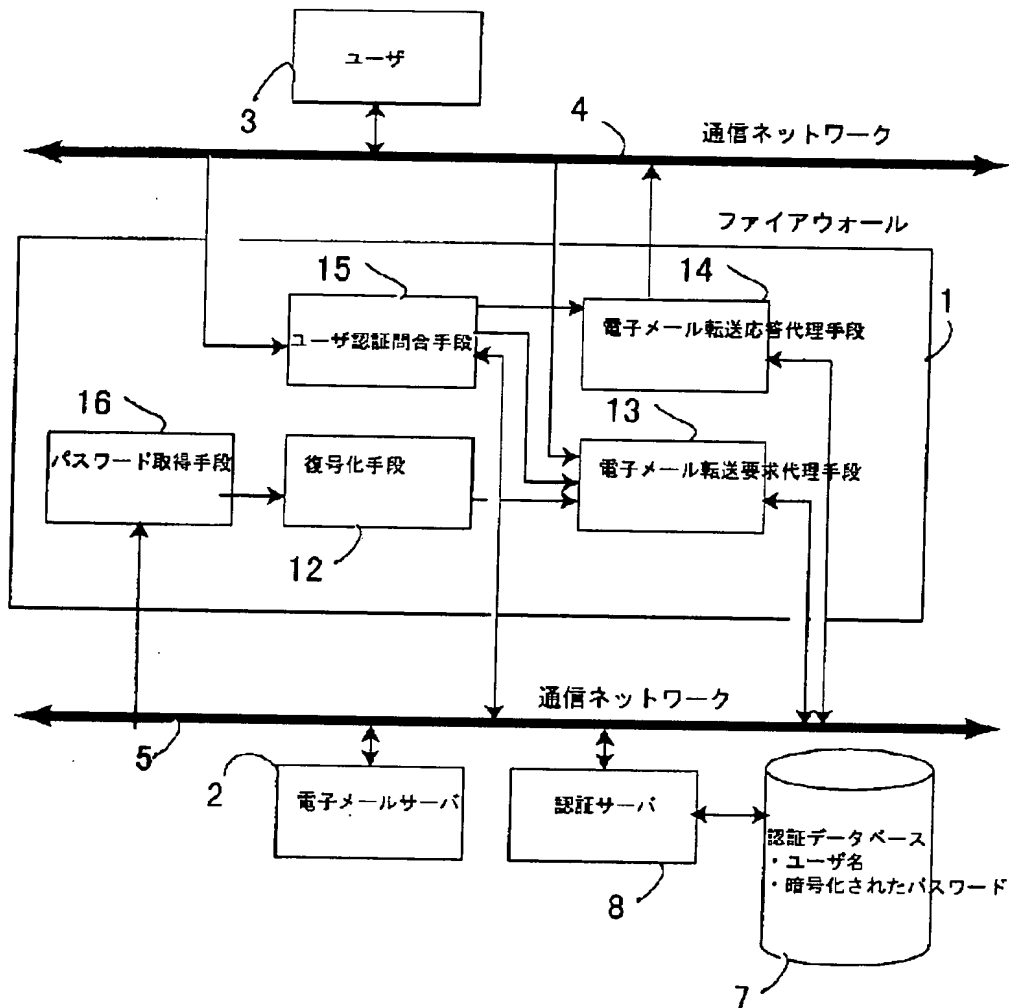
16

- 37 : 通信チャンネル
 38 : 通信チャンネル
 39 : インターネット
 40 : ワークステーション
 41 : CPU (マイクロプロセッサ)
 42 : 磁気ディスク装置
 43 : ランダムアクセスメモリ
 44 : ブートROM
 45 : イーサネットインターフェイス
 10 46 : イーサネットインターフェイス
 47 通信チャンネル
 48 通信チャンネル

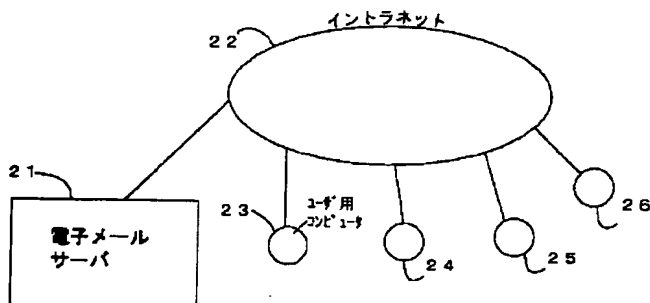
【図1】



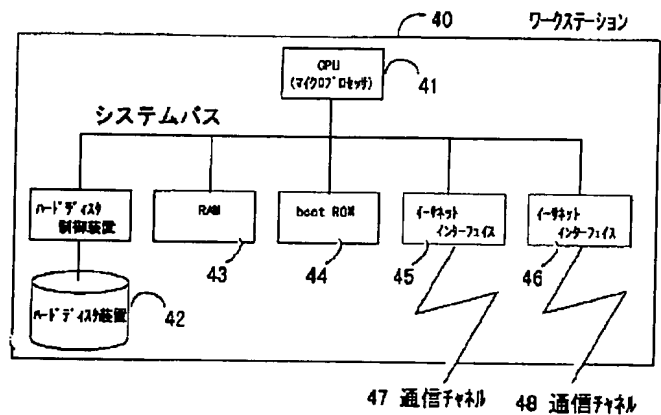
【図 2】



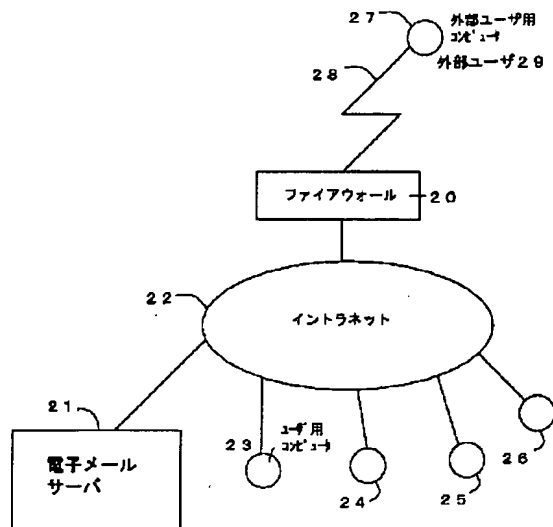
【図 3】



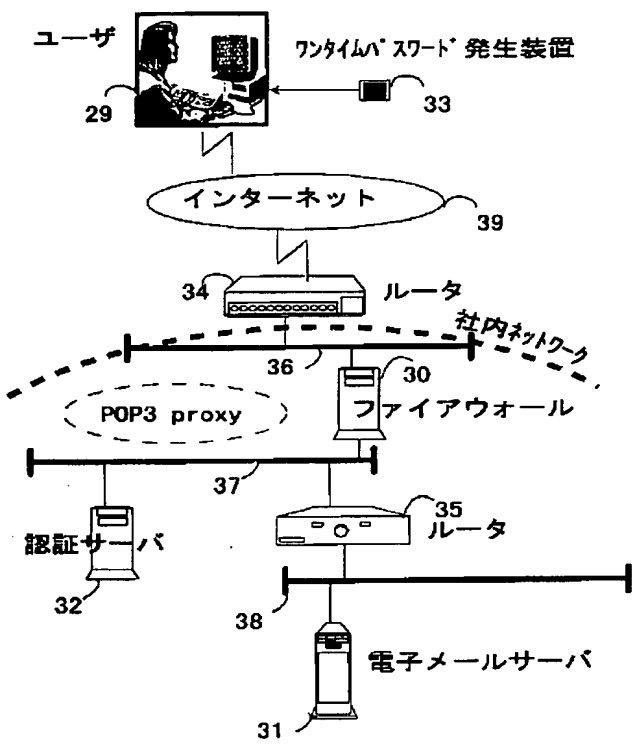
【図 6】



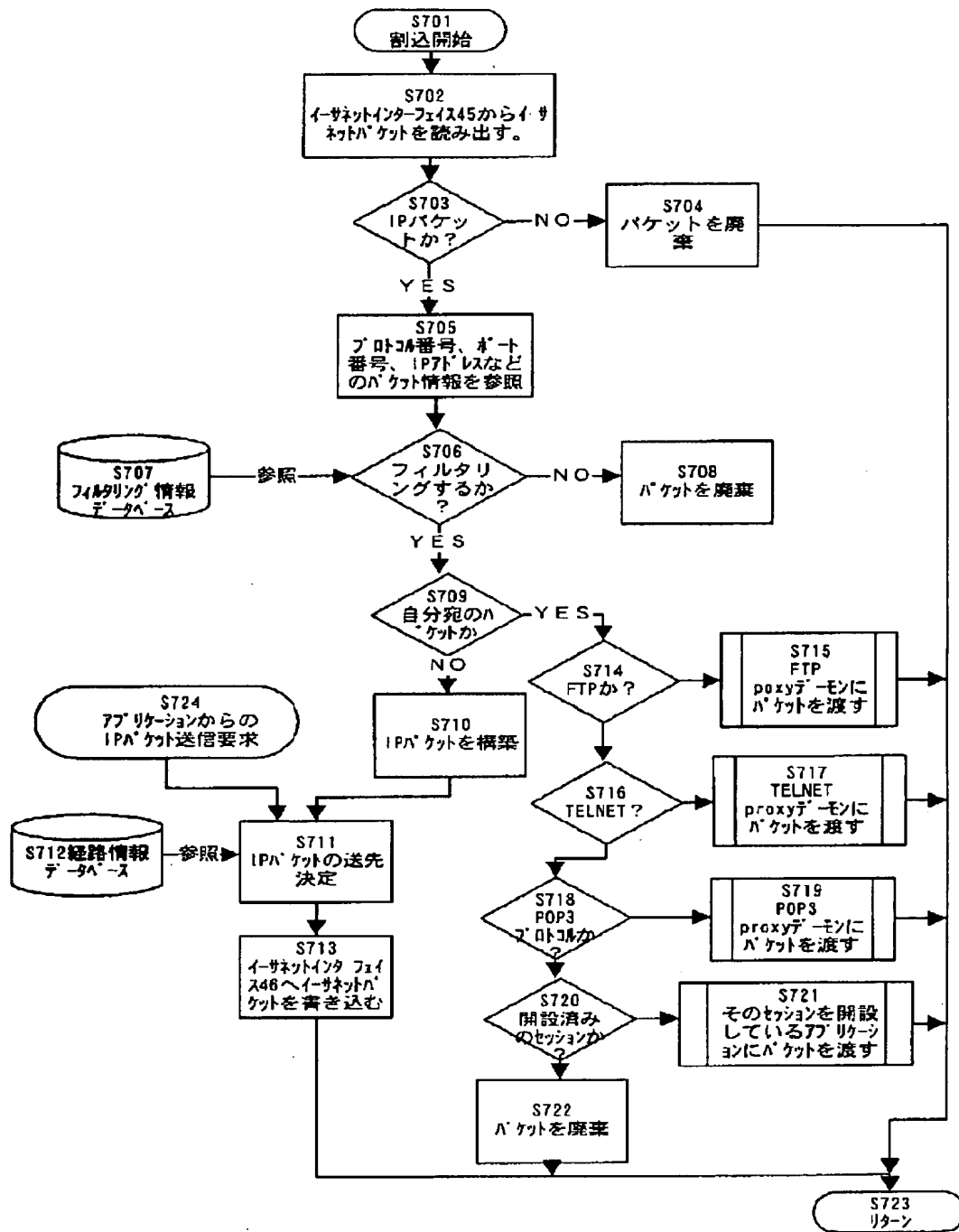
【図4】



【図5】



【図 7】



【図 8】

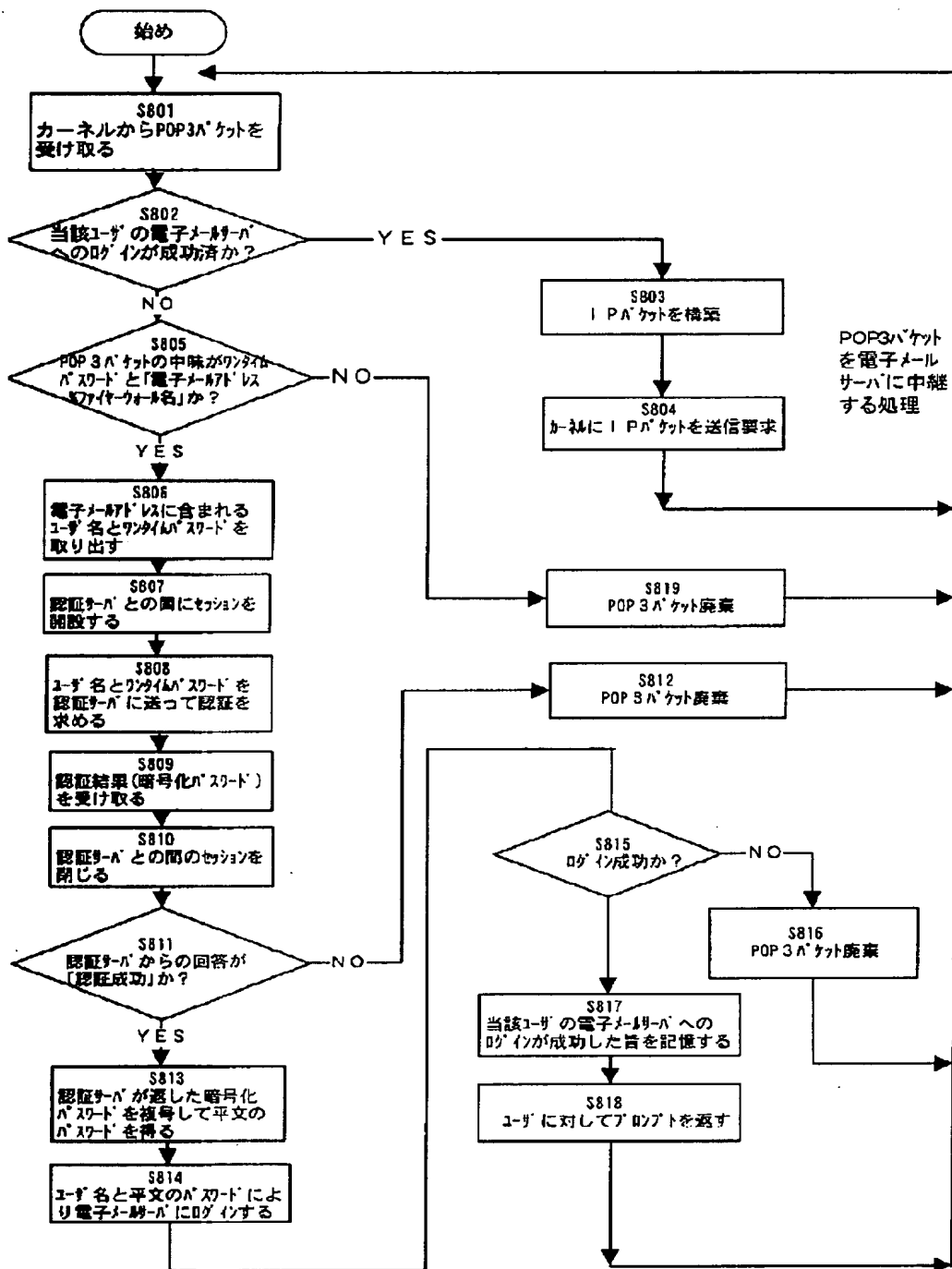


図 8 POP3 proxy による電子メール転送(外部通信ネットワーク → 内部通信ネットワーク)要求処理フロー
(外部ユーザからファイアウォールに対して要求したときの処理)

【図 9】

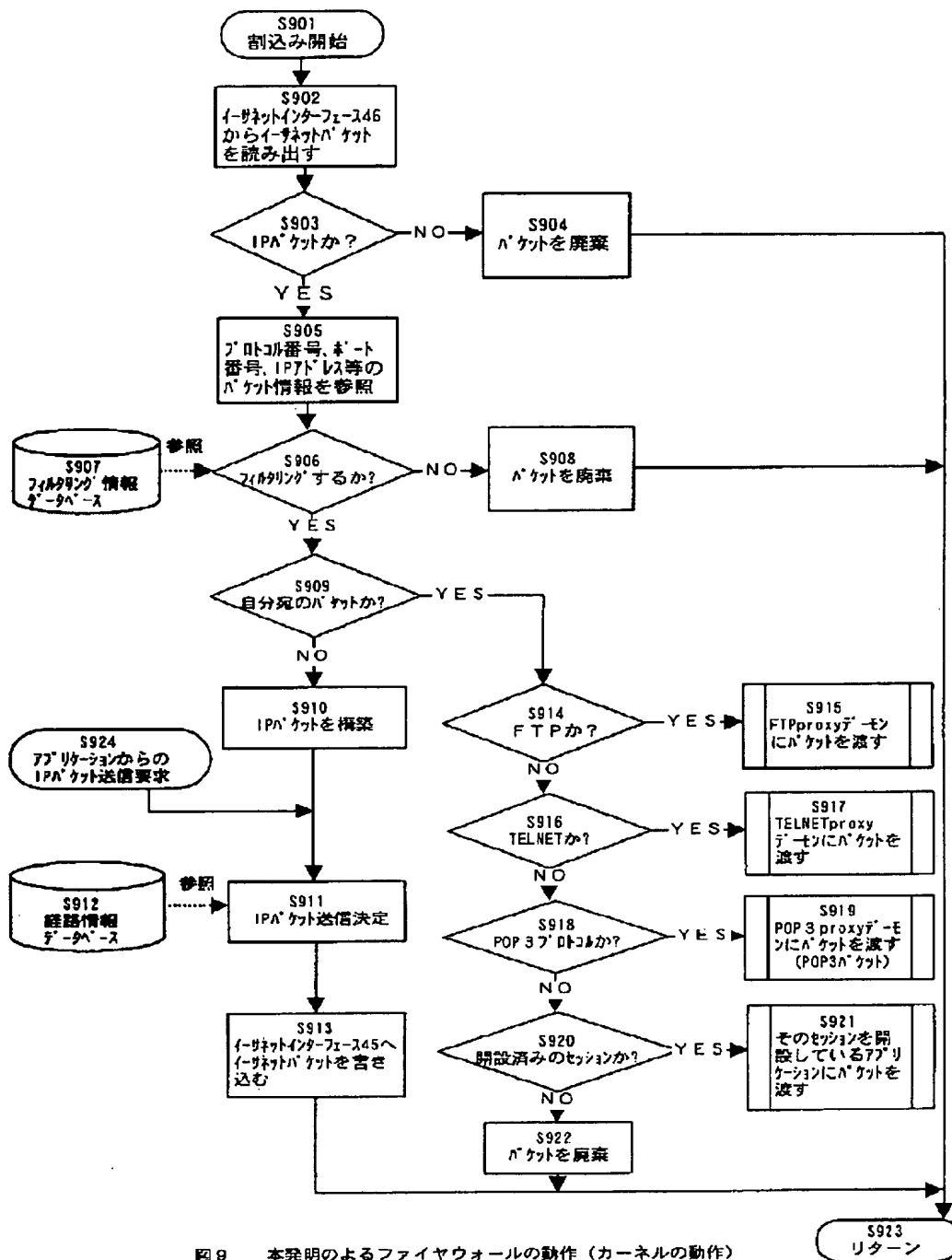


図9 本発明によるファイウォールの動作（カーネルの動作）

【図10】

